UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/821,079	03/29/2001	Messaoud Benantar	AUS920010064US1	5333

65362 7590 06/23/2008

HAMILTON & TERRILE, LLP
IBM Austin
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
BROWN, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/821,079
Filing Date: March 29, 2001
Appellant(s): BENANTAR, MESSAOUD

Michael Rocco Cannatti
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/16/08 appealing from the Office action mailed 11/01/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,892,307	WOOD	5-2005
5,892,828	PERLMAN	4-1999
6,640,141	OLDEN	10-2002
6,754,829	BUTT	6-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1, 3-6, 14, 16-19, 25, and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood US 6,892,307 in view of Perlman US 5,892,828.

As per claim 1, Wood teaches a method for an authentication process within a distributed data processing system, the method comprising: receiving an attribute certificate (credentials structure) (Col 18 lines 34-35) from a client (browser client) (Col 18 line 38) at a host (authentication service) (Col 18 line 50) within the distributed data processing system (enterprise system) (Col 7 lines 34-36); extracting encrypted authentication data from the attribute certificate (decrypting) (Col 18 lines 54-55), wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host (encrypted with public key of authentication service) (Col 18 lines 49-51); decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host (decrypting with using authentication service private key) (Col 18 lines 54-55). Wood fails to teach forwarding the authentication data to a controlled resource.

Perlman teaches forwarding the authentication data to a controlled resource which authenticates the client before allowing access. (Application 236 at Server Node 202b) (Col 6 lines 28-35).
It would have been obvious to one of ordinary skill in the art to use the forwarding of Perlman with the system of Wood to because forwarding allows authentication to various application in a distributed system, and the systems are in the analogous art of authentication.

As per claim 3, Wood teaches the authentication data comprises a user identity and a password (username password pair)(Claim 27).

As per claim 4, Perlman. teaches authenticating the client for access to the controlled resource based on the authentication data (efficient authentication), (Col 6 line 32-33).

As per claim 5, Wood teaches that the certificate (credential structure) (Col 18 line 35) contains multiple sets of authentication data (at least 2) (claim 27) for multiple hosts (plural information resources) (claim 24), the method further comprising: parsing the authentication data to retrieve a specific set of authentication data for the host (obtaining the credential) (claim 24).

As per claim 6 Wood teaches that the authentication data (credential structure) (Col 18 line 35) contains multiple sets of authentication parameters (at least 2) (claim 27) for multiple controlled resources (plural information resources) (claim 24), the method further comprising: parsing the authentication data to retrieve a specific set of authentication data for the controlled resource (obtaining the credential) (claim 24).

As per claim 14, Wood teaches a method for an authentication process within a distributed data processing system, the method comprising: receiving an attribute certificate (credentials structure) (Col 18 lines 34-35) from a client (browser client) (Col 18 line 38) at a host (authentication service) (Col 18 line 50) within the distributed data processing system (enterprise system) (Col 7 lines 34-36); extracting encrypted authentication data from the attribute certificate (decrypting) (Col 18 lines 54-55), wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host (encrypted with public key of authentication service) (Col 18 lines 49-51); decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host (decrypting with using authentication service private key) (Col 18 lines 54-55). Wood fails to teach forwarding the authentication data to a controlled resource.
Perlman teaches forwarding the authentication data to a controlled resource which authenticates the client before allowing access. (Application 236 at Server Node 202b) (Col 6 lines 28-35).
It would have been obvious to one of ordinary skill in the art to use the forwarding of Perlman with the system of Wood to because the systems are in the analogous art of authentication.

As per claim 16, Woods teaches the authentication data comprises a user identity and a password (username password pair)(Claim 27).

As per claim 17, Perlman. teaches authenticating the client for access to the controlled resource based on the authentication data (efficient authentication), (Col 6 line 32-33).

As per claim 18, Wood teaches that the certificate (credential structure) (Col 18 line 35) contains multiple sets of authentication data (at least 2) (claim 27) for multiple hosts (plural information

resources) (claim 24), the method further comprising: parsing the authentication data to retrieve a specific set of authentication data for the host (obtaining the credential) (claim 24).

As per claim 19 Wood teaches that the authentication data (credential structure) (Col 18 line 35) contains multiple sets of authentication parameters (at least 2) (claim 27) for multiple controlled resources (plural information resources) (claim 24), the method further comprising: parsing the authentication data to retrieve a specific set of authentication data for the controlled resource (obtaining the credential) (claim 24).

As per claim 25, Wood teaches a method for an authentication process within a distributed data processing system, the method comprising: receiving an attribute certificate (credentials structure) (Col 18 lines 34-35) from a client (browser client) (Col 18 line 38) at a host (authentication service) (Col 18 line 50) within the distributed data processing system (enterprise system) (Col 7 lines 34-36); extracting encrypted authentication data from the attribute certificate (decrypting) (Col 18 lines 54-55), wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host (encrypted with public key of authentication service) (Col 18 lines 49-51); decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host (decrypting with using authentication service private key) (Col 18 lines 54-55).
Wood fails to teach forwarding the authentication data to a controlled resource.
Perlman teaches forwarding the authentication data to a controlled resource which authenticates the client before allowing access. (Application 236 at Server Node 202b) (Col 6 lines 28-35).
It would have been obvious to one of ordinary skill in the art to use the forwarding of Perlman with the system of Wood to because the systems are in the analogous art of authentication.

As per claim 27, Wood teaches the authentication data comprises a user identity and a password (username password pair) (Claim 27).

As per claim 28, Perlman. teaches authenticating the client for access to the controlled resource based on the authentication data (efficient authentication), (Col 6 line 32-33).

As per claim 29, Wood teaches that the certificate (credential structure) (Col 18 line 35) contains multiple sets of authentication data (at least 2) (claim 27) for multiple hosts (plural information resources) (claim 24), the method further comprising: parsing the authentication data to retrieve a specific set of authentication data for the host (obtaining the credential) (claim 24).

As per claim 30 Wood teaches that the authentication data (credential structure) (Col 18 line 35) contains multiple sets of authentication parameters (at least 2) (claim 27) for multiple controlled resources (plural information resources) (claim 24), the method further comprising: parsing the authentication data to retrieve a specific set of authentication data for the controlled resource (obtaining the credential) (claim 24).

Claims 2, 15, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood US 6,892,307 in view of Perlman US 5,892,828 in view of Olden US 6,460,141

As per claims 2, 15, and 26 the previous Wood-Perlman combination does not teach legacy applications.

Olden teaches the controlled resource is a legacy application (legacy application) (Col 25 lines 20-25). It would have been obvious to one of ordinary skill in the art to use the legacy application of Olden with

the system of Wood-Perlman because it maintains backwards compatibility and they are of analogous arts.

Claim 7, 20, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood US 6,892,307 in view of Perlman US 5,892,828 in view of Butt US 6,754,829

As per claims 7, 20, and 31 the previous Wood-Perlman combination does not teach the X.509 standard. Butt teaches certificates are formatted according to an X.509 standard (X.509) (Col 4 lines 56-65).

It would have been obvious to one of ordinary skill in the art to use the X.509 standard because it is well known and operating system independent (Col 4 lines 60-65).

(10) Response to Argument

A. Claims 1, 3-6, 14, 16-19, 25, 27-30

Appellant argues that the Examiner has not met the claim limitations of claims 1, 14, and 25 because the examiner has relied on Wood column, 18, lines 35-55 to meet the limitation of "extracting" and "decrypting" the appellant argues that the two are distinct, and Wood only teaches decrypting.

The examiner points to Wood column 18 lines 35-55 and Figure 4. Wood teaches that a "credentials structure" 410, may contain several login credentials which are encrypted using a public key. Wood teaches that to recover the credentials they must be decrypted. The examiner argues that to decrypt the credentials, they must be extracted from the credentials structure, or vice versa, when the credentials are decrypted they are extracted from the credentials structure. One cannot decrypt without extracting the credentials, and one can't extract without decrypting. Thus Wood teaches both extracting and decrypting, where the login credentials structure meets the attribute certificate limitation of claims 1, 14, and 25.

Appellant argues that Perlman does not teach the authentication forwarding in the proper manner. The examiner admits that appellant's characterization of Perlman through steps 1-5 is correct. This can be best seen on Figure 2. However the examiner is not relying completely on Perlman authentication, but more for the structure of the authentication. Wood teaches a client being authenticated in order to reach a controlled resource as stated in claims 1, 14 and 15. What Wood does not teach is forwarding the authentication data to the controlled resource, so that the controlled resource for authentication. Perlman, Figure 2, Column 6 lines 28-35, and Steps 3-5 of the appellants' argument meet this limitation. Perlman is relied on because directory services 202a (client) sends authentication information to a workstation 210 (host) and the authentication information is decrypted, then the workstation 210 (host) forwards the authentication information to server node

202b, and application 236. The application then makes sure the authentication information is correct. Perlman is not needed for the actual Authentication just the structure for which the authentication takes place. Woods teaches a multi-step alternate authentication structure that authenticates "the client" (Column 11 line 52 to Column 12 line 65) . Perlman teaches a three party authentication where the information is sent from A, to B, to C as is stated in independent claims 1, 14, and 15. Thus the combination of Wood and Perlman meet the current claim limitations of forwarding authentication data to a controlled resource which authenticate the client based on the authentication data before allowing the client to access the controlled resource.

B. Claims 2, 15, and 26

Appellant relies on arguments regarding claims 1, 14, and 25 for claims 2, 15, and 26. Those arguments are addressed above.

C. Claims 7, 20, and 31

Appellant relies on arguments regarding claims 1, 14 and 25 for claims 7, 20, and 31. Those arguments are addressed above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Christopher J. Brown /Christopher J Brown/

Conferees:

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134